Security for Complex Systems

Definition of complex systems

Diverse kinds of entities tightly coupled. Codes, hardware, user, network. Can't worry about one aspect… creates blind spots.

Poorly defined perimeter.

System whose model is larger than what you can verify.

Complexity depends on the security property.
Only let in good people: Hard to define good people

Don't know the (security) policy.

What is security? For real systems?

Is the notion that security is a safety + liveness property good enough in practice?

(Fred pointed out that we should say "hyperproperties" during the presentation.)

How does a system behave in the presence of adversaries?

Complexity hurts completeness of proving/testing for security.

Uncertainty about the model.

Attacks predicated on what you have…if you don't know what you have may be attacker doesn't either. But attacker needs to only find one weakness… or is this really true? Can attacker attack key things using weakness? Obfuscation to the rescue?

Single application can be sufficiently complex. Simple properties of complex applications can be established by formal methods.
Type checking can help…
Properties defending against particular attacks

Decomposition: essential; decomposing in different ways. Solve toy problems and build up or how do we rebuild system to achieve security goals? Does your laptop have to be a general-purpose Turing Machine? Deal with complexity by eliminating it.

Do decomposition in a way that identifies all the real interfaces.

How well does model fit property? Side-channel attacks. More of a problem with complex systems. Bad guy finds flaw in our model before us.

Toxoplasmosis almost adversarial. Cats -> Humans -> Rodents… rodents become aggressive to feline.

Complex defense mechanisms can be turned against you.

Robustness requires complexity that leads to fragility.

Take into account dynamics of system.

Suggestions:

Control complexity: Design to test; design for security diagnostics.

Do we have to start anew or can we remove complexity from existing systems?
Nobody in the Federal Government has the authority to simplify systems!

Can we start by creating little islands? Need to work with legacy systems.
Adaptability of systems.

What are the complexity that we can handle? Can we reduce to manageable levels… OS kernet ->Hypervisor -> mini-Hypervisor

Can't always design for predictable responses?

Operations research

Immune response systems reacting to pathogens: Models may be useful.
Continuing to operate while you are being attacked. Responding and learning from the attack. Defense in depth: Native immunity, adaptive immunity… wall-like defenses; nimble defenses. Antigen library. Protein shape space is very limited (especially for the signaling part). Look for bacterial functional part that have no mammalian analog.
Fixed points in architectures (waist of hourglass) not mutable and antibiotics can attack those. Can we use symbionts to help in the fight against pathogens?

Computer Science analogy: Users encouraged to be part of the immune system response.